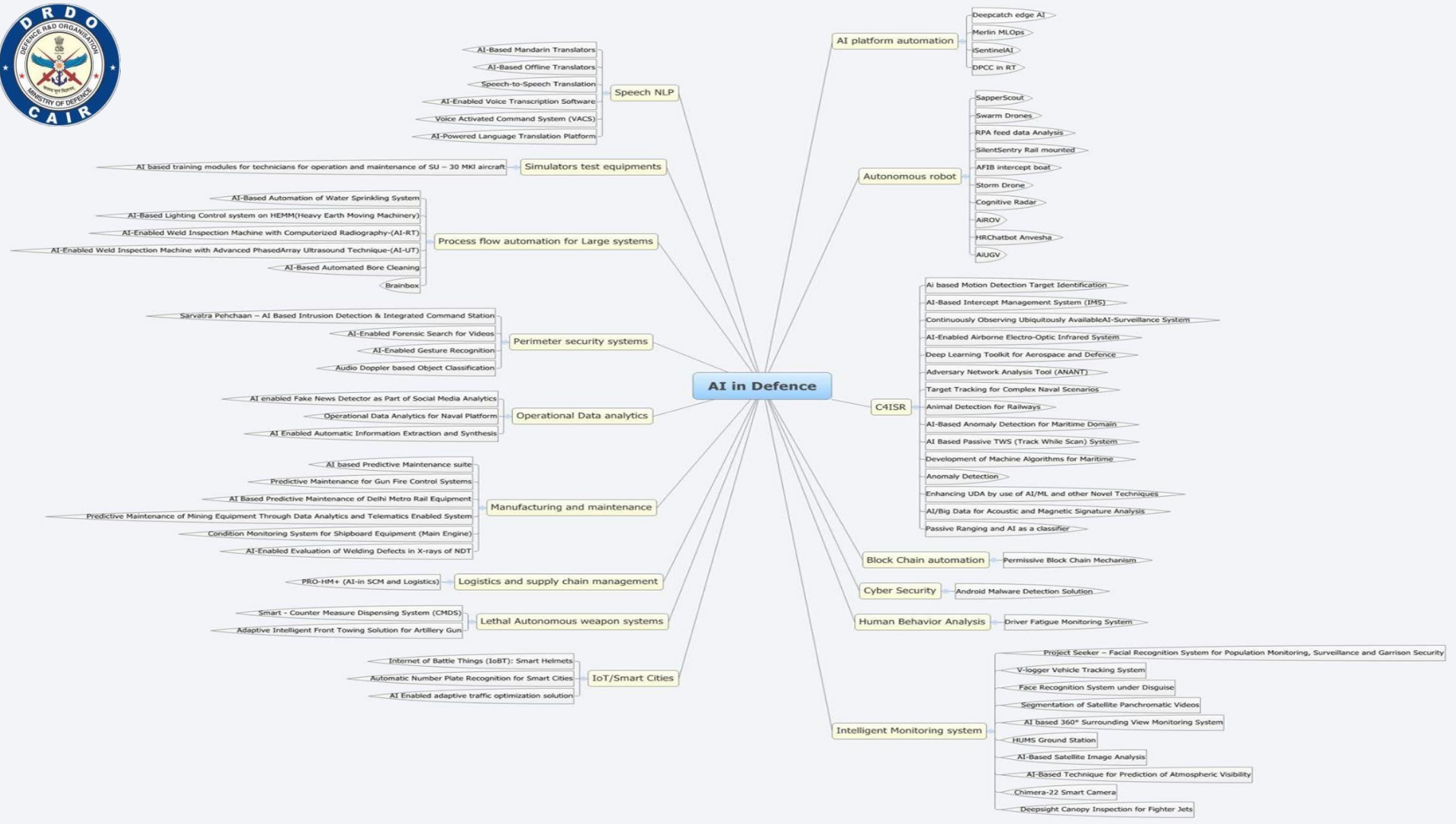

# AI in Defence Systems

## Performance Enhancing Technology

Loveneet Kumar, Sc E
CAIR, DRDO, Bangalore


AI in Defence
AI platform automation
Deepcatch edge AI
Merlin MLOps
iSentinelAI
DPCC in RT
Autonomous robot
SapperScout
Swarm Drones
RPA feed data Analysis
SilentSentry Rail mounted
AFIB intercept boat
Storm Drone
Cognitive Radar
AiROV
HRChatbot Anvesha
AiUGV
C4ISR
Ai based Motion Detection Target Identification
AI-Based Intercept Management System (IMS)
Continuously Observing Ubiquitously AvailableAI-Surveillance System
AI-Enabled Airborne Electro-Optic Infrared System
Deep Learning Toolkit for Aerospace and Defence
Adversary Network Analysis Tool (ANANT)
Target Tracking for Complex Naval Scenarios
Animal Detection for Railways
AI-Based Anomaly Detection for Maritime Domain
AI Based Passive TWS (Track While Scan) System
Development of Machine Algorithms for Maritime
Anomaly Detection
Enhancing UDA by use of AI/ML and other Novel Techniques
AI/Big Data for Acoustic and Magnetic Signature Analysis
Passive Ranging and AI as a classifier
Block Chain automation
Permissive Block Chain Mechanism
Cyber Security
Android Malware Detection Solution
Human Behavior Analysis
Driver Fatigue Monitoring System
Intelligent Monitoring system
Project Seeker – Facial Recognition System for Population Monitoring, Surveillance and Garrison Security
V-logger Vehicle Tracking System
Face Recognition System under Disguise
Segmentation of Satellite Panchromatic Videos
AI based 360° Surrounding View Monitoring System
HUMS Ground Station
AI-Based Satellite Image Analysis
AI-Based Technique for Prediction of Atmospheric Visibility
Chimera-22 Smart Camera
Deepsight Canopy Inspection for Fighter Jets
Speech NLP
AI-Based Mandarin Translators
AI-Based Offline Translators
Speech-to-Speech Translation
AI-Enabled Voice Transcription Software
Voice Activated Command System (VACS)
AI-Powered Language Translation Platform
Simulators test equipments
AI based training modules for technicians for operation and maintenance of SU – 30 MKI aircraft
Process flow automation for Large systems
AI-Based Automation of Water Sprinkling System
AI-Based Lighting Control system on HEMM(Heavy Earth Moving Machinery)
AI-Enabled Weld Inspection Machine with Computerized Radiography-(AI-RT)
AI-Enabled Weld Inspection Machine with Advanced PhasedArray Ultrasound Technique-(AI-UT)
AI-Based Automated Bore Cleaning
Brainbox
Perimeter security systems
Sarvatra Pehchaan – AI Based Intrusion Detection & Integrated Command Station
AI-Enabled Forensic Search for Videos
AI-Enabled Gesture Recognition
Audio Doppler based Object Classification
Operational Data analytics
AI enabled Fake News Detector as Part of Social Media Analytics
Operational Data Analytics for Naval Platform
AI Enabled Automatic Information Extraction and Synthesis
Manufacturing and maintenance
AI based Predictive Maintenance suite
Predictive Maintenance for Gun Fire Control Systems
AI Based Predictive Maintenance of Delhi Metro Rail Equipment
Predictive Maintenance of Mining Equipment Through Data Analytics and Telematics Enabled System
Condition Monitoring System for Shipboard Equipment (Main Engine)
AI-Enabled Evaluation of Welding Defects in X-rays of NDT
Logistics and supply chain management
PRO-HM+ (AI-in SCM and Logistics)
Lethal Autonomous weapon systems
Smart - Counter Measure Dispensing System (CMDS)
Adaptive Intelligent Front Towing Solution for Artillery Gun
IoT/Smart Cities
Internet of Battle Things (IoBT): Smart Helmets
Automatic Number Plate Recognition for Smart Cities
AI Enabled adaptive traffic optimization solution

# What is Performance in Defence?

**Performance in Defence is measured by several key factors:**

- **Decision Speed:** *The rapidness of assessment and response.*
- **Target Accuracy:** *The precision and effectiveness of engagement.*
- **Survivability:** *The ability of forces and systems to endure threats.*
- **Operational Readiness:** *The state of being prepared for immediate deployment.*
- **Resource Efficiency:** *The optimal use of available personnel and materials.*
- **Strategic Deterrence:** *The capacity to dissuade adversarial actions.*

**AI is not adopted because it is modern. It is adopted because it enhances performance.**

# From Platform Superiority to Algorithmic Superiority

**Traditional:**

Bigger tanks, faster jets

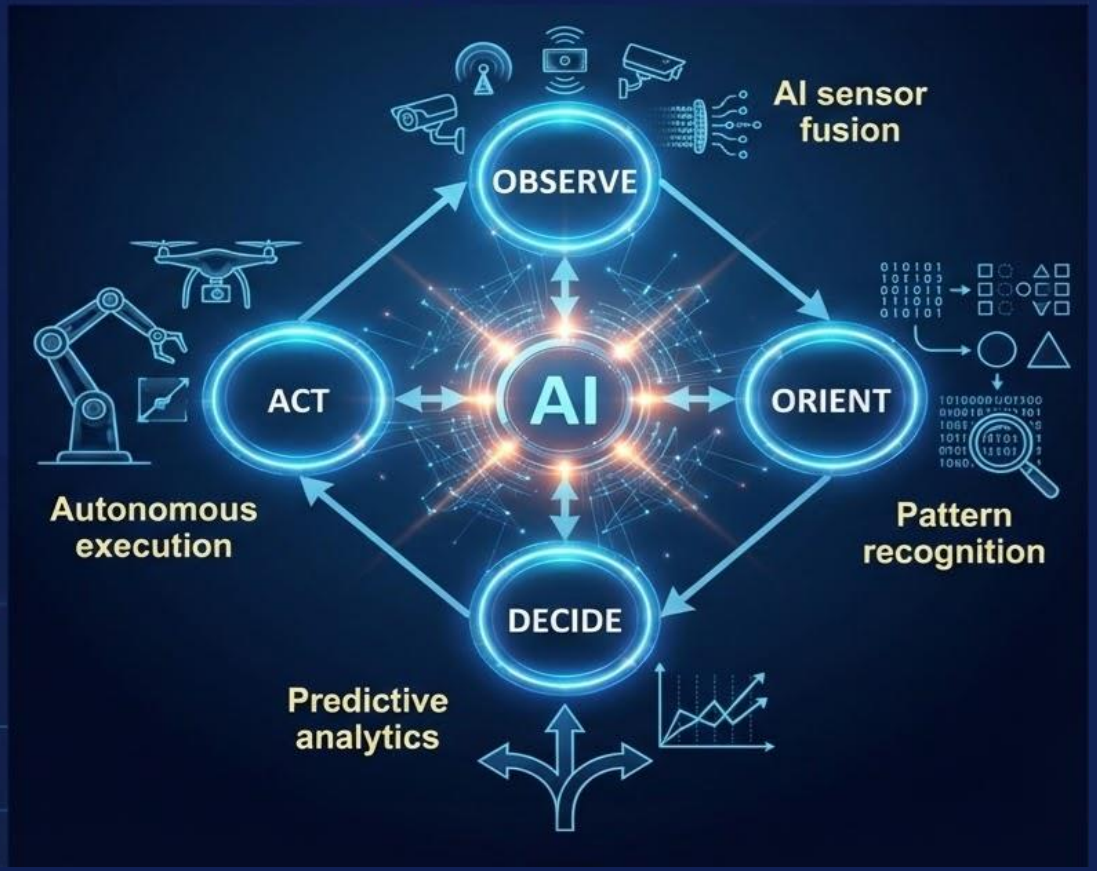
**Now:**

Faster computation, smarter models

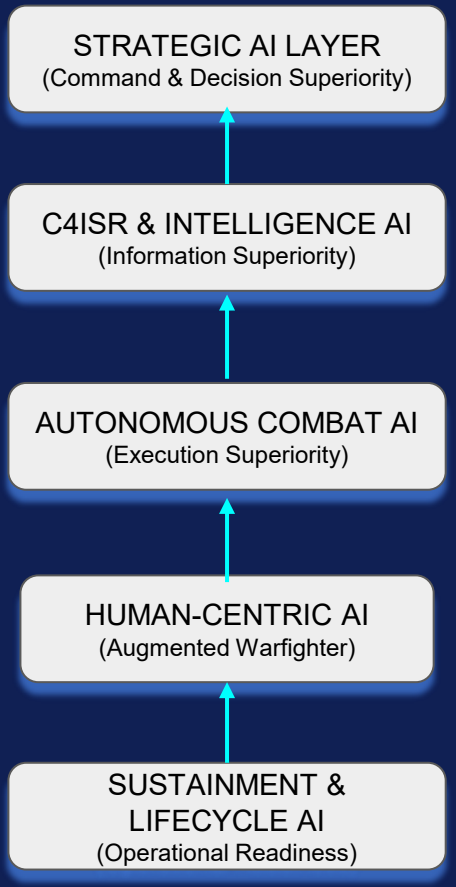
# MACHINE PERFORMANCE ENHANCEMENT

# AI in the OODA Loop

- **Observe** *AI sensor fusion*
- **Orient** *Pattern recognition*
- **Decide** *Predictive analytics*
- **Act** *Autonomous execution*



# Integrated AI-Enabled Defence Performance Architecture




## AI Assurance & Validation Framework

***Explainability***

***Robustness***

***Adversarial Resilience***

***Bias Mitigation***

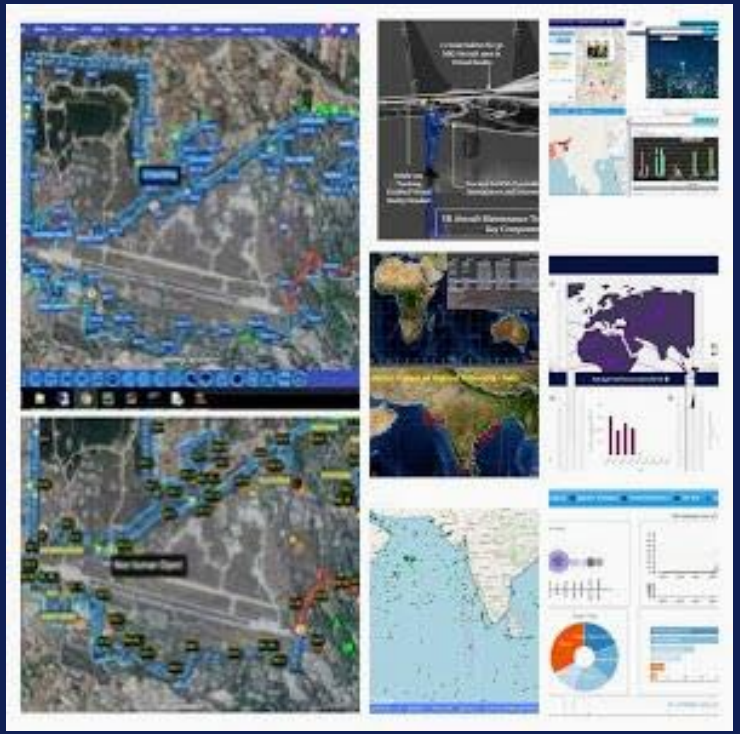
***Human Oversight***

***Continuous Monitoring***

# STRATEGIC AI LAYER

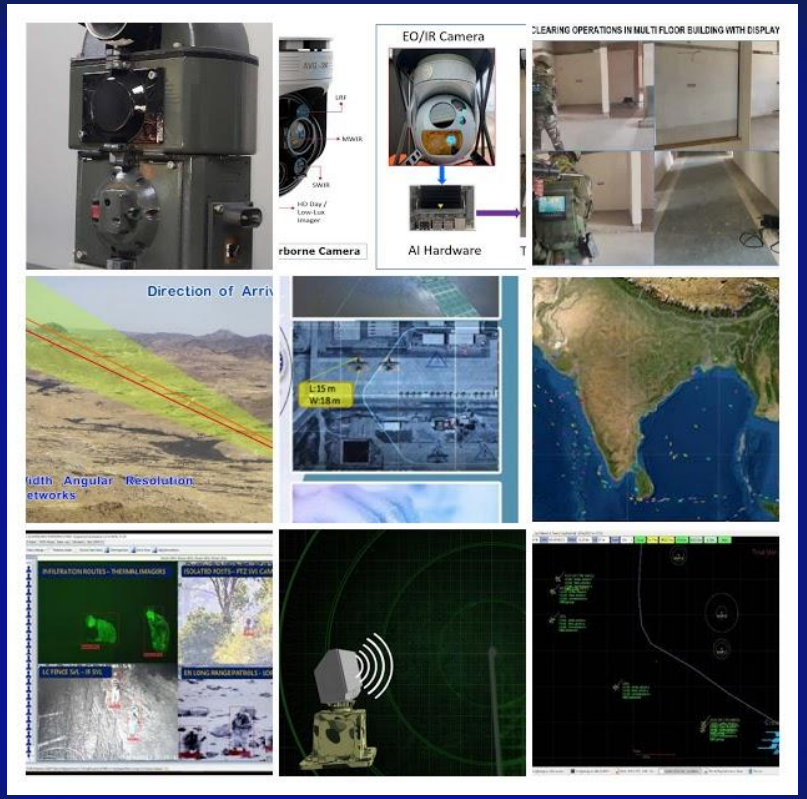
**Command & Decision Superiority**

- **AI-driven decision support**
- **War-gaming & scenario simulation**
- **Threat forecasting & escalation modelling**



# C4ISR Performance Gains

- Faster target detection
- Reduced false positives
- Real-time anomaly detection
- Enhanced situational awareness

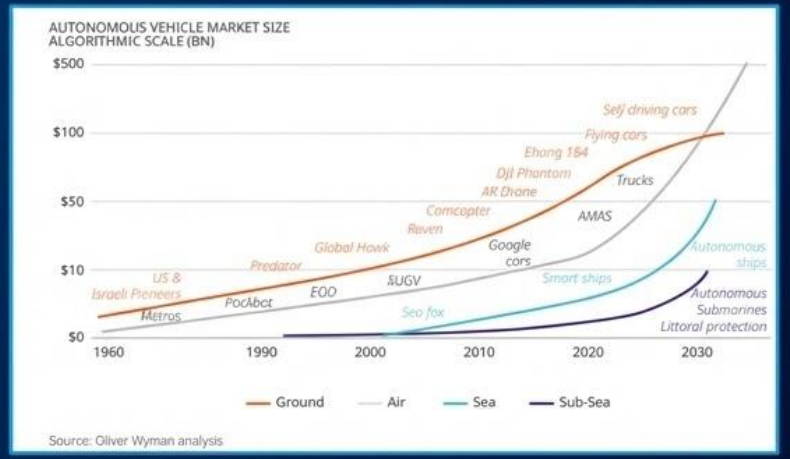
# Autonomous Systems as Force Multipliers

**Performance gains:**

- **Risk reduction**
- **Scalability**
- **Faster response**
- **Lower cost per mission**

| Type of UAV | Cost per flight hour | Procurement cost |
|---|---|---|
| Light tactical | 6% | 8% |
| MALE | 17% | 22% |
| HALE | 47% | 70% |

Source: Oliver Wyman analysis




Source: Oliver Wyman analysis

Technology on The Battlefield, Oliver Wyman,2025

# Swarm Intelligence

**Performance enhancement:**

- **Saturation capability**
- **Redundancy**
- **Distributed decision-making**

# Lifecycle Performance

**AI improves:**

- Fleet availability
- Maintenance prediction
- Spare forecasting
- Logistics optimisation


**Readiness is performance**

# HUMAN PERFORMANCE ENHANCEMENT

# The Augmented Soldier

## Cognitive capacity

- Smart Helmet & Real-Time Mapping
- Faster threat detection
- GPS-denied navigation
- Team awareness

## Perceptual range

- Voice & NLP Systems
- Reduced cognitive load
- Faster command input
- Multilingual intelligence processing

## Endurance

- Human exoskeleton & Fatigue Monitoring
- Reduced accident rate
- Improved mission endurance
- Predictive risk mitigation
- Performance Drugs Discovery

# TRUSTWORTHY AI AS A PERFORMANCE REQUIREMENT

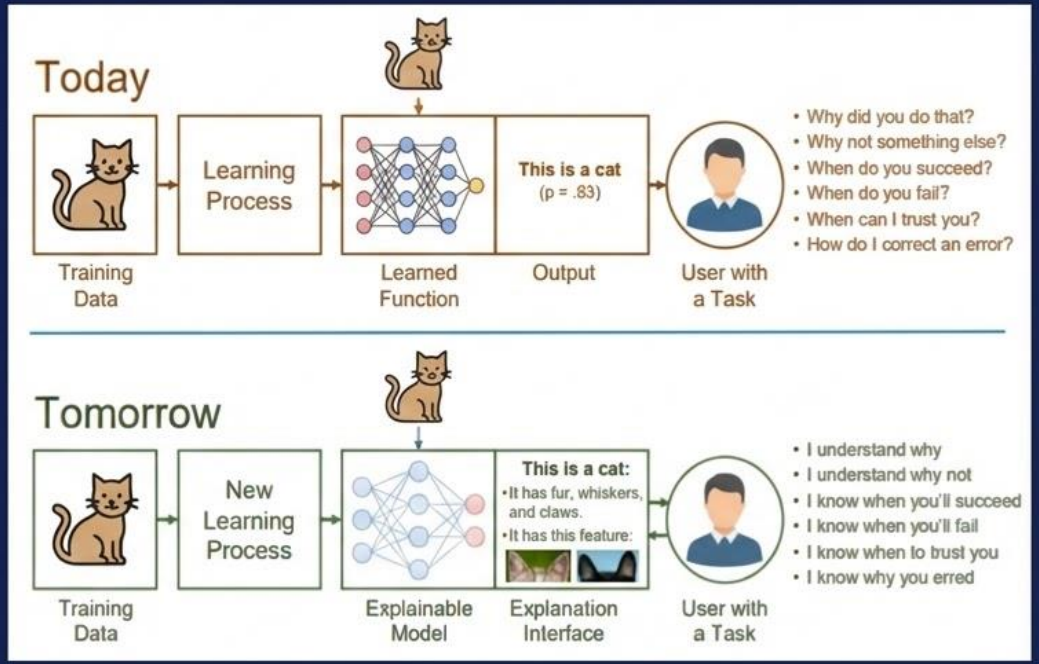
When AI Decides

*Performance Depends on Trust*

# Explainability Enhances Performance

**Explainability Enhances Performance**

- **Faster operator confidence**
- **Reduced hesitation**
- **Improved human-AI teaming**
- **Better post-mission analysis**




**Explainable AI improves operational tempo.**

# Adversarial Attacks Degrade Performance

**Examples:**

- **Camouflage causing misclassification**
- **GPS spoofing**
- **Radar spoofing**

**Impact:**

- **False targeting**
- **Operational confusion**

**Robust AI protects performance.**

| Modality & type of Perturbations | Attack Techniques | Attack-Type | Defences |
|---|---|---|---|
| **Image** - Manipulating pixels to cause misclassification | - Query-based attacks (ZOO attack, Boundary attack, Square attack)<br>- Transferability attacks | Black-Box | - Adversarial Training<br>- Input Transformation (e.g., JPEG compression)<br>- Defensive Distillation |
| **Image** - Manipulating pixels with full model knowledge | - Fast Gradient Sign Method (FGSM)<br>- Projected Gradient Descent (PGD)<br>- Carlini & Wagner attacks | White-Box | - Adversarial Training<br>- Gradient Masking<br>- Robust Optimization |
| **Text** - Altering words to deceive models | - Synonym substitution<br>- Text perturbation | Black-Box | - Adversarial Training<br>- Text Augmentation<br>- Defensive Distillation |
| **Text** - Modifying text with full model knowledge | - Gradient-based attacks<br>- HotFlip | White-Box | - Adversarial Training<br>- Gradient Masking<br>- Robust Optimization |
| **Audio** - Adding noise to mislead models | - Audio perturbation<br>- Frequency manipulation | Black-Box | - Adversarial Training<br>- Input Transformation (e.g., noise reduction)<br>- Defensive Distillation |
| **Audio** - Manipulating audio with full model knowledge | - Gradient-based attacks<br>- Psychoacoustic hiding | White-Box | - Adversarial Training<br>- Gradient Masking<br>- Robust Optimization |
| **Tabular Data** - Modifying entries to deceive models | - Query-based attacks<br>- Feature manipulation | Black-Box | - Adversarial Training<br>- Data Sanitization<br>- Defensive Distillation |
| **Tabular Data** - Altering features with full model knowledge | - Gradient-based attacks<br>- Feature perturbation | White-Box | - Adversarial Training<br>- Gradient Masking<br>- Robust Optimization |

| Poisoning Level | Attack Techniques | Attack-Type | Defences |
|---|---|---|---|
| **Data: Corrupting training data** | - Label Manipulation<br>- Backdoor Attacks<br>- Noise Injection<br>- Data Injection<br>- Label Flipping<br>- Grammar and Style Alteration | Both (White-Box and Black-Box) | - Data Sanitization<br>- Robust Training<br>- Anomaly Detection<br>- Data Validation and Cleaning<br>- Content Filtering |
| **Algorithm: Manipulating the training algorithm** | - Algorithm Tampering<br>- Hyperparameter Manipulation | White-Box | - Algorithm Verification<br>- Secure Development Practices |
| **Model: Compromising model parameters** | - Parameter Injection<br>- Model Trojaning<br>- Architecture Modification | White-Box | - Model Validation<br>- Secure Model Training<br>- Ensemble Analysis<br>- Model Pruning<br>- Parameter Monitoring |

| Type of Attack | Attack Techniques | Attack Type | Defences |
|---|---|---|---|
| **Model Inversion Attack** | - Reconstructing input data from model outputs | Both (Black-Box and White-Box) | - Differential Privacy<br>- Homomorphic Encryption<br>- SMC |
| **Membership Inference Attack** | - Determining if a input data was in the training set | Both (Black-Box and White-Box) | - Differential Privacy<br>- Access Control Mechanisms<br>- SMC |
| **Model Extraction Attack** | - Replicating model functionality through extensive querying | Both (Black-Box and White-Box) | - Rate Limiting<br>- API Security<br>- Obfuscation |

# Bias Reduces Operational Effectiveness

**Examples:**

- **Terrain bias**
- **Language bias**
- **Population bias**

**Impact:**

- **Misidentification**
- **False alarms**
- **Theatre-specific failures**

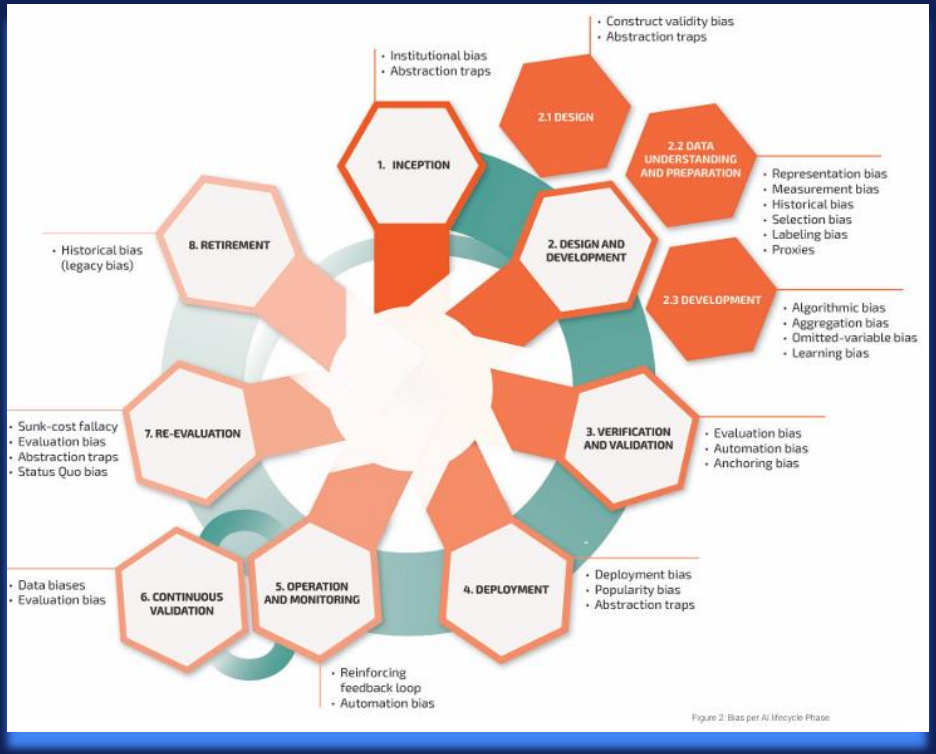
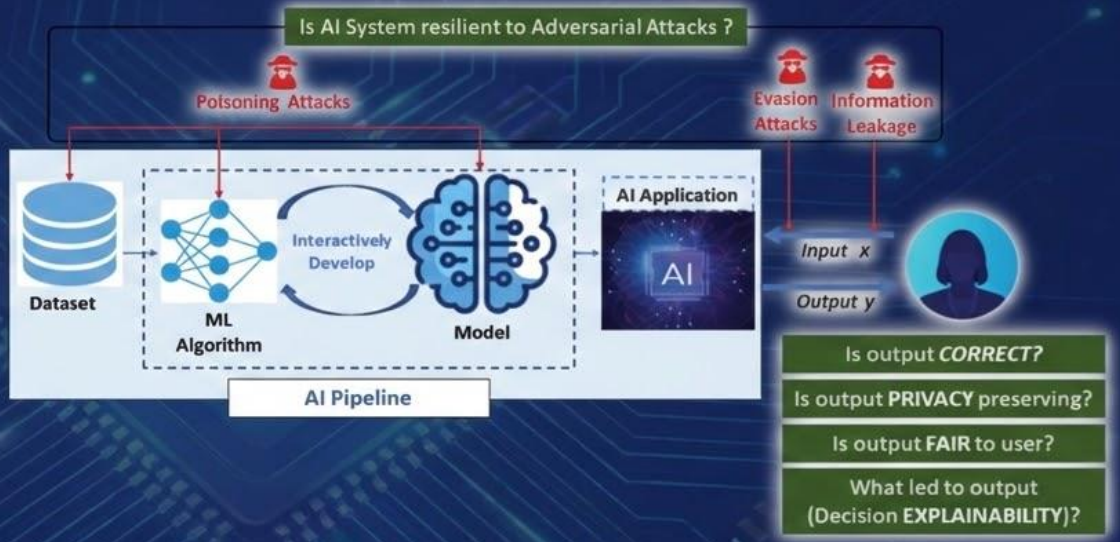



Image Source: "From Inception to Retirement: Addressing Bias Throughout the Lifecycle of AI Systems A Practical Guide", Suzanne Snoek, Isabel Barberá ,2024

# Trustworthiness as a Performance Multiplier

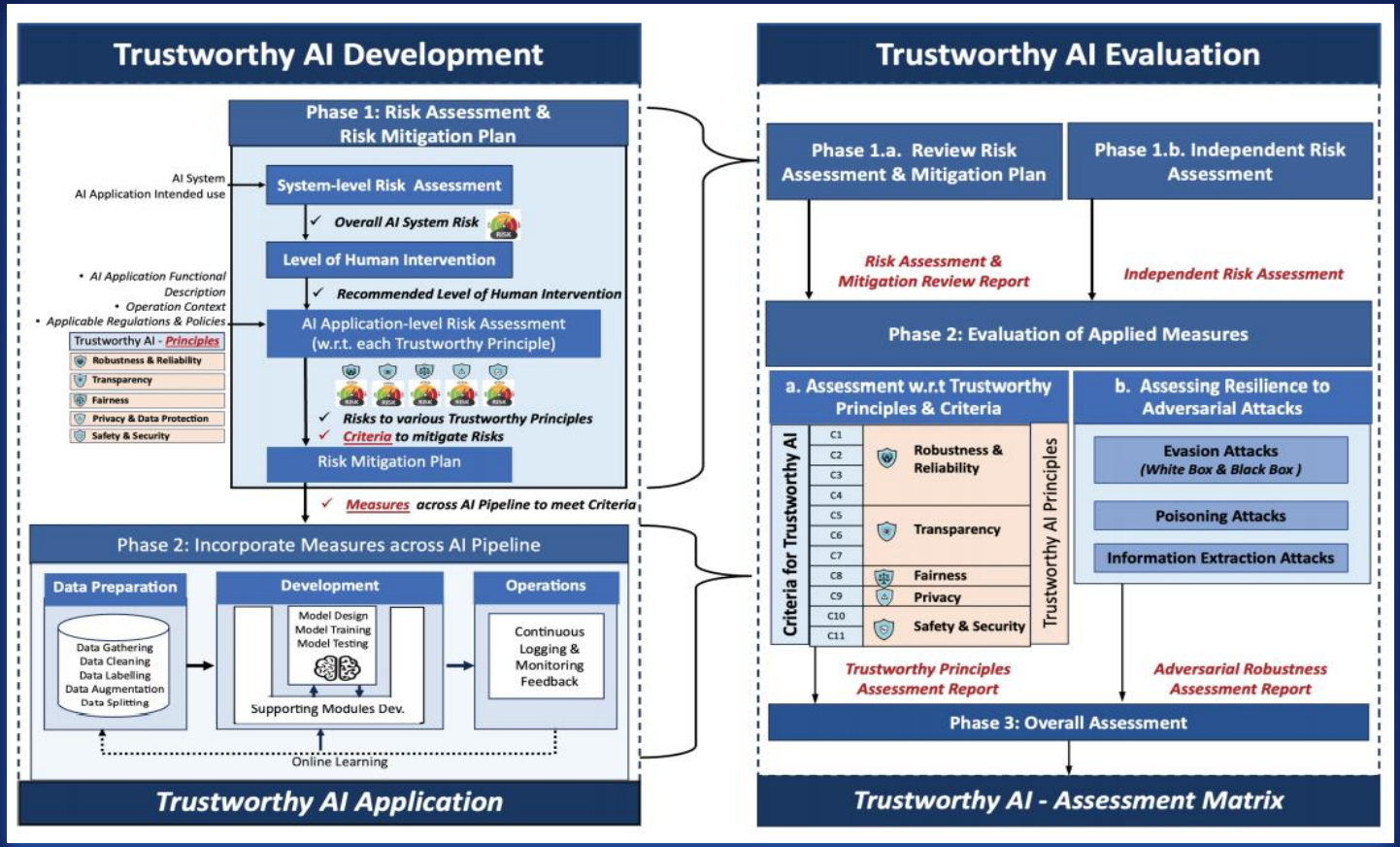
**Dimensions:**

- **Robustness**
- **Reliability**
- **Transparency**
- **Security**
- **Human oversight**




**Without these *Performance collapses*.**

# Developing Performance-Grade Trustworthy AI




Source: "Evaluating Trustworthy AI (ETAI) Framework for Defence". DRDO (Oct 2024)

# Indigenous AI Systems Enhancing Performance

**National Performance Advantage**

- Swarm drones
- Predictive maintenance suite
- AI translators
- HUMS

**Indigenisation improves:**

- Supply chain resilience
- Rapid iteration
- Custom theatre optimisation

# FUTURE PERFORMANCE LANDSCAPE

**Performance will depend on:**

Processing power & efficiency

***Algorithm speed***

***Swarm dominance***

Coordinated autonomous systems

***AI logistics***

Optimized supply chains

***Cognitive command centres***

Integrated decision-making

AI enhances Machines, Humans, Systems, Logistics, Strategy


But only if it is trustworthy.

# THANK YOU

AI in defence is not about replacing soldiers.

It is about Enhancing Performance — Responsibly, Reliably, and Strategically.